At step **618**, smartcard **90** similarly computes the SAKh using the SAK and the PN. This value is then stored in non-volatile memory. The GPS timestamp may also be stored in memory. This completes the mating process. Upon completion of the process, communication between STB **80** and smartcard **90** is protected by using the SAK or the SAKh for authentication.

Although the invention has been described in terms of the illustrative embodiment, it will be appreciated by those skilled in the art that various changes and modifications may be made to the illustrative embodiment without departing from the spirit or scope of the invention. For example, the SMK could be omitted from the above-described embodiment. In such an embodiment, the SAK would be directly encrypted under the SPK. It is intended that the scope of the invention not be limited in any way to the illustrative embodiments shown and described but that the invention be limited only by the claims appended hereto. For example, the present invention is not limited to a cable system, either but may be applicable to satellite, streaming media, etc.

What is claimed is:

1. A system for securely providing the same authentication key to components of a communication network, the system comprising:

a) an authentication key;

b) a first key for encrypting the authentication key;

c) a set-top box for deriving the authentication key using the first key;

d) a second key for encrypting the authentication key and for encrypting the first key;

e) a smartcard for deriving the authentication key using the second key;

f) a third key for encrypting the first key, the first key being encrypted by the smartcard, and being forwarded to the set-top box; and

g) the set-top box receiving the encrypted first key and extracting said first key using the third key, wherein the third key is held by the set-top box and is used for deriving the authentication key wherein the authentication key uniquely mates the smartcard to the set-top box.

2. The system of claim **1** wherein the first key is extracted from the encrypted first key by the smartcard prior to f).

3. The system of claim **1** wherein the authentication key is for authenticating communication from the set-top box to the smartcard, and for encrypting communication from the smartcard to the set-top box.

4. The system of claim **1** further comprising a protocol nonce for determining a hashed authentication key using the authentication key.

5. The system of claim **4** wherein the set-top box and the smartcard both compute the hashed authentication key for storage in respective memory.

6. The system of claim **5** wherein the hashed authentication key is for authenticating communication between the smartcard and the set-top box.

7. The system of claim **6** wherein the third key is forwarded by the set-top to the smartcard.

8. The system of claim **7** wherein the third key is encrypted with the smartcard's public key.

9. The system of claim **1** wherein the second key is stored within a memory of the smartcard at the time of manufacture.

10. The system of claim **9** further comprising a conditional access system, communicably coupled to the set-top box, for transmitting the first key encrypted by the second key.

11. The system of claim **10** wherein the smartcard derives the first key by using the second key stored in the memory.

12. A method for securely providing the same authentication key to a signal-receiving apparatus as well as to a token communicably coupled to signal-receiving apparatus, the method comprising:

a) receiving a first message comprising the authentication key encrypted by a first key;

b) receiving a second message comprising the authentication key encrypted by a second key;

c) receiving a third message comprising the first key encrypted by the second key;

d) using the token to derive the first key from the third message, the first key being derived by the second key;

e) using the token to derive the authentication key from the second message, the authentication key being derived by the second key;

f) using a third key for encrypting the first key to form a fourth message, the first key being encrypted by the token;

g) forwarding the fourth message to the signal-receiving apparatus;

h) using the third key for deriving the first key, the third key being held by the signal-receiving apparatus and the first key being derived by the signal-receiving apparatus; and

i) using the signal-receiving apparatus to derive the authentication key from the first message, the authentication key being derived with the first key wherein the authentication key uniquely mates the smartcard to the set-top box.

13. The method of claim **12** further comprising determining a hashed authentication key using a protocol nonce.

14. The method of claim **13** further comprising authenticating communication between the token and the signal-receiving apparatus, the communication being authenticated with the hashed authentication key.

15. The method of claim **12** further comprising

storing the second key in a memory of the token prior to steps d) and e).

16. The method of claim **12** further comprising

storing the authentication key in the signal-receiving apparatus; and

storing the authentication key in the token.

17. The method of claim **12**, wherein the fourth message is generated by the token.

* * * * *